Title (en)

METHOD FOR DETECTING ABNORMALITIES IN A CRYPTOGRAPHIC CIRCUIT PROTECTED BY DIFFERENTIAL LOGIC, AND CIRCUIT FOR IMPLEMENTING SAID METHOD

Title (de)

VERFAHREN FÜR DEN NACHWEIS VON ANOMALIEN IN EINER DURCH DIFFERENZIELLE LOGIK GESCHÜTZTEN KRYPTOGRAFISCHEN SCHALTUNG UND SCHALTUNG ZUR UMSETZUNG DIESES VERFAHRENS

Title (fr)

PROCEDE DE DETECTION D'ANOMALIES DANS UN CIRCUIT DE CRYPTOGRAPHIE PROTEGE PAR LOGIQUE DIFFERENTIELLE ET CIRCUIT METTANT EN OEUVRE UN TEL PROCEDE

Publication

EP 2324442 B1 20120208 (FR)

Application

EP 09806408 A 20090730

Priority

- EP 2009059886 W 20090730
- FR 0855537 A 20080812

Abstract (en)

[origin: WO2010018071A1] The invention relates to a method for detecting abnormalities in a circuit protected by differential logic and processing logic variables represented by a pair of components (at, af), a first network of cells (T) carrying out logic functions on the first component of said pairs, a second network of dual cells (F) operating as a complementary logic on the second component, the logic functions being carried out by each pair of cells (T, F) in a preload phase (21) placing the variables in a known state at the cell input, followed by an evaluation phase (22) in which a calculation is carried out by the cells, wherein said method is characterised in that an abnormality is detected by at least one inconsistency state. The invention also relates to a circuit protected by differential logic, comprising means for testing the consistency of the two components of the logic variables during the preload or evaluation phases at the monitored nodes of the circuit.

IPC 8 full level

G06F 21/55 (2013.01); **G06F 21/75** (2013.01)

CPC (source: EP KR US)

G06F 21/55 (2013.01 - KR); **G06F 21/602** (2013.01 - KR); **G06F 21/755** (2017.07 - EP KR US)

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

DOCDB simple family (publication)

WO 2010018071 A1 20100218; AT E545095 T1 20120215; CA 2733667 A1 20100218; CA 2733667 C 20171107; CN 102124470 A 20110713; CN 102124470 B 20150408; EP 2324442 A1 20110525; EP 2324442 B1 20120208; ES 2386061 T3 20120808; FR 2935059 A1 20100219; FR 2935059 B1 20120511; JP 2012505563 A 20120301; JP 5891562 B2 20160323; KR 101722790 B1 20170405; KR 20110083591 A 20110720; US 2012124680 A1 20120517; US 8955160 B2 20150210

DOCDB simple family (application)

EP 2009059886 W 20090730; AT 09806408 T 20090730; CA 2733667 A 20090730; CN 200980131525 A 20090730; EP 09806408 A 20090730; ES 09806408 T 20090730; FR 0855537 A 20080812; JP 2011522468 A 20090730; KR 20117003337 A 20090730; US 200913058706 A 20090730